



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/690,243	10/17/2000	Ari Engelberg	36530/RRT/S850	2962
23363 7590 10/09/2007 CHRISTIE, PARKER & HALE, LLP PO BOX 7068 PASADENA, CA 91109-7068			EXAMINER ELISCA, PIERRE E	
			ART UNIT 3621	PAPER NUMBER
			MAIL DATE 10/09/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/690,243

Applicant(s)

ENGELBERG ET AL.

Examiner

Pierre E. Elisca

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on RCE7/30/2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 and 10-79 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8 and 10-79 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>4/07 and 7/07</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This communication is in response to Applicant's RCE filed on 07/30/2007.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-8 and 10-79 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whitehouse (U.S. Patent No. 6,005,945 (*applicant submitted IDS*) in view of Pang et al (U.S. Patent No 6,446,204).

4. As per claim 1, Whitehouse teaches a on-line system for printing value bearing items a client system and a server comprising a database remote from the client system and including information about a plurality of users, a plurality of security device transaction data records stored in the database to ensure authenticity of the plurality of users (*see figs 3, 4, column 7 line 54-8 line 11 also see fig 4, column 8 lines 23-29, 54-58, 9 line 15-19*). Whitehouse fail to teach scalable server system capable of communicating with the client system over a communication network wherein the scalable server system is configured to process each security device transaction data record can be processed in a

stateless manner; an a stateless cryptographic module to authenticate the users using the plurality of security device transaction data records stored in the database. However, Pang et al teach scalable server system capable of communicating with the client system over a communication network wherein the scalable server system is configured to process each security device transaction data record can be processed in a stateless manner; an a stateless cryptographic module to authenticate the users using the plurality of security device transaction data records stored in the database (*see abstract, figs 2, 6 and 8, column 23 lines 26-64, 25 lines 1-20*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Whitehouse et al. disclosure to include Pang et al scalable server system capable of communicating with the client system over a communication network wherein the scalable server system is configured to process each security device transaction data record can be processed in a stateless manner; an a stateless cryptographic module to authenticate the users using the plurality of security device transaction data records stored in the database because this would have ensure that client would be properly authenticate whenever service is needed thereby enhance the flexibility of the system.

5. As per claim 2, Whitehouse teaches a system wherein each security device transaction data is related to a user (*see column 9 lines 12-20*).

6. As per claim 3, Whitehouse teaches a system wherein the security device transaction data related to a user is loaded into the cryptographic module when the user requests to operate on a value bearing item (*see column 9 lines 45-50*).

7. As per claim 4, Whitehouse teaches a system wherein the security device transaction data related to a user is updated and returned to the database (*see column 9 line 51-63, 12 line 53-56*).

8. As per claim 5, Whitehouse teaches a system further comprising one module is capable of processing any of the plurality of security device transaction data (*see column 9 line 51-63*).

9. As per claim 6, Whitehouse teaches a system wherein a user can be authenticated using any of the cryptographic modules (*see column 9 line 51-63*).

10. As per claim 7, Whitehouse teaches a system further comprising computer executable code for load-balancing to route user requests to the at least one more cryptographic module (*see column 19 line 35-20 line 8*).

11. As per claim 8, Whitehouse teaches a system further comprising computer executable code for load-balancing to distribute traffic among the multiple cryptographic modules (*see column 19 line 35-20 line 8*).

Art Unit: 3621

12. As per claim 10, Whitehouse teaches a system wherein the database is partitioned across a plurality of physical databases (*see fig 7*).

13. As per claim 11, Whitehouse teaches a system wherein the cryptographic module performs cryptographic function on a transaction related to the database (*see fig 7*).

14. As per claim 12, Whitehouse teaches a system further comprising computer executable code for password authentication to prevent unauthorized access to the database (*see column 10 line 45-60*).

15. As per claim 13, Whitehouse teaches a system wherein the database stores a first set of one or more last database transactions and the cryptographic module stores a second set of one or more last database transactions for comparison with the first set of one or more last database transactions stored in the database to verify each database transaction (*see column 8 line 63-9 line 12*).

16. As per claim 14, Whitehouse teaches a system wherein the cryptographic module prevents further database transactions if the second set of one or more last transaction stored in the cryptographic module does not compare with the first set of one or more last transaction stored in the database (*see column 9 lines 1-12*).

Art Unit: 3621

17. As per claim 15, Whitehouse teaches a system wherein the cryptographic module includes a data validation subsystem for allowing the module to verify that data is up to date and an auto-recovery subsystem for automatically re-synchronize the module with the data (*see column 9 line 32-50*).

18. As per claim 16, Whitehouse teaches a system wherein the cryptographic module includes a computer executable code for preventing unauthorized modification of data (*see column 15 line 1-17*).

19. As per claim 17, Whitehouse teaches a system wherein the cryptographic module includes a computer executable code for ensuring the proper operation of cryptographic security and VBI related meter functions (*see column 16 line 45-67*).

20. As per claim 18, Whitehouse teaches a system wherein the cryptographic module includes a computer executable code for supporting multiple concurrent users (*see fig 7*).

21. As per claim 19, Whitehouse teaches a system wherein the database includes one or more indicium data elements, data for account maintenance, and data for revenue protection (*see fig 4*).

Art Unit: 3621

22. As per claim 20 and 21, Whitehouse teaches a system wherein the database includes virtual meter information and a descending register data (see *column 10 line 50-11 line 26, 14 lines 25-36*).

23. As per claims 22 and 23, Whitehouse teaches a system wherein the value bearing item is a mail piece that comprises a digital signature (see *column 7 lines 1-5, 8 line 47-51 and 11 lines 27-29*).

24. As per claim 24, Whitehouse teaches a system wherein the cryptographic module performs cryptographic function on validation information according to a user request for printing a VBI (see *column 9 lines 12-30*).

25. As per claim 25, Whitehouse teaches a system wherein the cryptographic module generates data sufficient to print a postal indicium in compliance with postal service regulation on a mail piece (see *column 8 line 65-9 line 11*).

26. As per claims 26-31, Whitehouse teaches a system wherein a bar code is printed on the value bearing item that is a ticket, is a coupon, is currency, a voucher, a traveler's check (see *column 8 lines 14-18, 13 lines 56-60*).

27. As per claim 32, Whitehouse teaches a system wherein each security device transaction data includes one or more of an ascending register value, a descending register value, a respective cryptographic module ID, an indicium key

Art Unit: 3621

certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective module, expiration dates for keys, and a passphrase repetition list (*see column 9 lines 12-67, 13 lines 20-36, 14 lines 25-55*).

28. As per claim 33, Whitehouse teaches a system wherein each security device transaction data includes one or more of a private key, a public key, and a public key certificate, wherein the private key is used to sign module status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the module and the VBI are authentic (*see column 9 lines 12-50, 13 lines 20-36*).

29. As per claim 34, Whitehouse teaches a system wherein the cryptographic module is capable of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms (*see column 23 lines 49-59*).

30. As per claim 35, Whitehouse teaches a system wherein the server system further comprises one or more of a postal server subsystem, a provider server subsystem, an e-commerce subsystem, a staging subsystem, a client support subsystem, a decision support subsystem, a SMTP subsystem, an address

Art Unit: 3621

matching service subsystem, a SSL proxy server subsystem, and a web server subsystem (*see figs 3 and 4*).

31. As per claim 36, Whitehouse teaches a system wherein the database includes one or more of a postal database, a provider database, an e-commerce database, and a membership database (*see fig 3, 4*).

32. As per claim 37, Whitehouse teaches a system further comprising an address matching server for verifying a correct address specified by a user (*see column 12 line 65-13 line 15*).

33. As per claim 38, Whitehouse teaches a system further comprising a printer driver database for storing supported printer driver information (*see figs 3 and 4*).

34. As per claim 39, Whitehouse teach a method for printing value-beating items (VBI) via a communication network including a client system and a server system the method comprising accepting print requests from one or more users by the client system, communicating the print requests to the server system over the communication network, storing in a database a plurality of security device transaction data records, ensuring authenticity of the one or more users, utilizing a respective security device transaction data record (*see figs 3, 4, column 7 line 54-8 line 11 also see fig 4, column 8 lines 23-29, 54-58, 9 line 15-19*).

Whitehouse fail to teach a system for processing in a stateless manner each security device transaction data record in the server system and authenticating by a scalable cryptographic module the one or more users utilizing one or more of the plurality of security device transaction data record stored in the database.. However, Pang et al teach a system for processing in a stateless manner each security device transaction data record in the server system and authenticating by a scalable cryptographic module the one or more users utilizing one or more of the plurality of security device transaction data record stored in the database (see abstract, *figs 2, 6 and 8, column 23 lines 26-64, 25 lines 1-20*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Whitehouse et al's invention to include Pangs et al's system for processing in a stateless manner each security device transaction data record in the server system and authenticating by a scalable cryptographic module the one or more users utilizing one or more of the plurality of security device transaction data record stored in the database because this would have ensure that client would be properly authenticate whenever service is needed thereby enhance the flexibility of the system

35. As per claim 40, Whitehouse teaches a method wherein each security device transaction data is related to a user (*see column 9 lines 12-20*).

Art Unit: 3621

36. As per claim 41, Whitehouse teaches a method further comprising of loading the security device transaction data related to a user into the cryptographic module when the user requests to operate value bearing item (see *column 9 lines 45-50*).

37. As per claim 42, Whitehouse teaches a method further comprising of updating and returning the security device transaction data related to a user to the database (see *column 9 line 51-63, 12 line 53-56*).

38. As per claim 43, Whitehouse teaches a method further comprising adding at least one more stateless cryptographic module, wherein each cryptographic module is capable of processing any of the plurality of security device transaction data (see *column 9 line 51-63*).

39. As per claim 44, Whitehouse teaches a method further comprising of authenticating a user using any of the cryptographic modules (see *column 9 line 51-63*).

40. As per claim 45, Whitehouse teaches a method further comprising load-balancing to route user requests to the at least one more cryptographic module see *column 19 line 35-20 line 8*).

41. As per claim 46, Whitehouse teaches a method further comprising load-balancing to distribute traffic among the multiple cryptographic modules see *column 19 line 35-20 line 8*).

42. As per claim 47, Whitehouse teaches a method further comprising authenticating any of the one or more users using the cryptographic module (see *column 9 line 51-63*).

43. As per claim 48, Whitehouse teaches a method comprising partitioning the database across a plurality of physical databases (see *fig 7*).

44. As per claim 49, Whitehouse teaches a method further comprising encrypting database transactions using the cryptographic module (see *column 10 line 45-60*).

45. As per claim 50, Whitehouse teaches a method further comprising verifying a user password before granting access to the database (see *column 15 line 1-17*).

46. As per claim 51, Whitehouse teaches a method further comprising storing one or more last database transactions in the database storing one or more last database transactions in the cryptographic module; and comparing the one or more last database transactions stored in the database with the one or more last

Art Unit: 3621

database transactions stored in the cryptographic module to verify each database transaction (*see column 16 line 45-67*).

47. As per claim 52, Whitehouse teaches a method further comprising encrypting transactions related to the database using the cryptographic module (*see column 15 line 1-17*).

48. As per claim 53, Whitehouse teaches a method further comprising storing one or more last database transactions in the database, storing one or more last database transactions in the cryptographic module for comparison with the one or more last database transactions stored in the database to verify each database transaction (*see column 10 line 45-60*).

49. As per claim 54, Whitehouse teaches a method further comprising preventing further database transactions if the one or more last transaction stored in the cryptographic module does not compare with the one or more last transaction stored in the database (*see column 8 line 63-9 line 12*).

50. As per claim 55, Whitehouse teaches a method further comprising preventing unauthorized modification of data using the cryptographic module (*see column 16 line 45-67*).

Art Unit: 3621

51. As per claim 56, Whitehouse teaches a method further comprising verifying that the database is up to date (*see column 10 line 45-60*).

52. As per claim 57, Whitehouse teaches a method further comprising automatically re-synchronizing the cryptographic module with the database (*see column 9 line 51-63*).

53. As per claim 58, Whitehouse teaches a method further comprising ensuring the proper operation of cryptographic security and VBI related meter functions (*see column 9 lines 12-20*).

54. As per claim 59, Whitehouse teaches a method further comprising supporting multiple concurrent operators (*see fig 7*).

55. As per claim 60, Whitehouse teaches a method further comprising storing information about a number of last transactions in a respective internal register of each of the one or more cryptographic devices, storing a table including the information about a last transaction in the database, comparing the information saved in the respective device with the respective information saved in the database; and loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database (*see column 10 line 45-11 line 25*).

Art Unit: 3621

56. As per claim 61, Whitehouse teaches a method further comprising the step of storing data for creating one or more indicium, account maintenance, and revenue protection (*see column 10 line 45-11 line 25*).

57. As per claims 62-65, Whitehouse teaches a method further comprising printing a mail piece includes a digital signature, a postage amount, an ascending register of used postage and descending register of available postage (*see column 13 lines 20-40, 14 line 25-36, 16 lines 19-38*).

58. As per claims 66-71, Whitehouse teaches a method further comprising printing a ticket, a bar code, a coupon, currency, a voucher, a traveler's check (*see column 7 line 46-53, 8 line 14-18, 13 lines 56-60*).

59. As per claim 72, Whitehouse teaches a method wherein the security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list (*see column 13 lines 20-40, 14 line 25-36, 16 lines 19-38*).

Art Unit: 3621

60. As per claim 73, Whitehouse teaches a method further comprising performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-I, and Pseudo-random number generation algorithms using each of the cryptographic devices (*see 23 lines 49-59*).

61. As per claim 74, Whitehouse teaches a method further comprising keeping track of user accesses to a vendor website using a website database (*see fig 7*).

62. As per claim 75, Whitehouse teaches a method further comprising storing postal transaction data, financial transaction data, customer marketing information, commerce product information, meter license information, meter resets, meter history, and meter movement information in an offline database (*see column 10 line 45- 11 line 29*).

63. As per claim 76, Whitehouse teaches a method further comprising storing customer information, financial transactions, and information for marketing queries in a data warehouse database (*see column 9 lines 12-31*).

64. As per claim 77, Whitehouse teaches a method further comprising authorizing and capturing funds from a customer's account and transferring the

Art Unit: 3621

funds to a vendor's account using an e-commerce server (*see column 11 line 60-67*).

65. As per claim 78, Whitehouse teaches a method further comprising verifying a correct address specified using a user using an address matching server (*see column 9 line 51-63, 12 line 53-56*).

As per claim 79, Whitehouse teaches a method further comprising storing supported printer driver information in a printer driver database (*see figs 3 and 4*).

RESPONSE TO ARGUMENTS

66. Applicant's arguments with respect to claims 1-8 and 10-79 have been considered but are not persuasive.

REMARKS

67. In response to Applicant's filed on 07/30/2007, Applicant argues that the prior art of record (Whitehouse 945" and Pang 204") fail to teach:

a. a stateless cryptographic module to authenticate any of the plurality of users using one or more of the plurality of security device transaction data records of stored in the database, in a stateless manner". As indicated above, the Examiner believes that Whitehouse fail to teach scalable server system capable of communicating with the client system over a communication network wherein

Art Unit: 3621

the scalable server system is configured to process each security device transaction data record can be processed in a stateless manner; an a stateless cryptographic module to authenticate the users using the plurality of security device transaction data records stored in the database. However, Pang et al teach scalable server system capable of communicating with the client system over a communication network wherein the scalable server system is configured to process each security device transaction data record can be processed in a stateless manner; an a stateless cryptographic module to authenticate the users using the plurality of security device transaction data records stored in the database (*see abstract, figs 2, 6 and 8, column 23 lines 26-64, 25 lines 1-20*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Whitehouse et al. disclosure to include Pang et al scalable server system capable of communicating with the client system over a communication network wherein the scalable server system is configured to process each security device transaction data record can be processed in a stateless manner; an a stateless cryptographic module to authenticate the users using the plurality of security device transaction data records stored in the database because this would have ensure that client would be properly authenticate whenever service is needed thereby enhance the flexibility of the system.

b. Applicant further argues that there is any disclosure in Pang about the authentication engines 802, 804, and 806 being stateless and being able to authenticate. However, the Examiner respectfully disagrees with Applicant's

Art Unit: 3621

characterization of the prior art. Pang discloses a distributed application server that provides for extensible authentication mechanism in a stateless web environment (see., figs 7A, 7B, and fig 8, the system of Pang, fig 8 has been performed in a stateless web environment, and therefore, Applicant argument is moot).

Conclusion


68. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pierre E. Elisca whose telephone number is 571 272 6706. The examiner can normally be reached on 6:30 to 5:00. Patents and hoteling.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on 571 272 6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 3621

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

September 26, 2007



PIERRE EDDY ELISCA
PRIMARY EXAMINER
TECHNOLOGY CENTER 3600